

HOMEWORK 1

DUE 14 JANUARY 2015

SHOW ALL YOUR WORK**1.** Compute

- (a) $7^{286} \pmod{13}$.
- (b) $6^{441} \pmod{19}$.
- (c) $6^{441} \pmod{65}$.

2. Only two of the following problems can be solved using the algorithm from the first lecture. Determine which ones and do them using said algorithm. For the other two, explain which of the necessary hypotheses is not satisfied.

- (a) Find the fifth root $\sqrt[5]{3}$ of 3 in arithmetic modulo 23.
- (b) Find the fifth root $\sqrt[5]{7}$ of 7 in arithmetic modulo 31.
- (c) Find the cube root $\sqrt[3]{4}$ of 4 in arithmetic modulo 57.
- (d) Find the cube root $\sqrt[3]{4}$ of 4 in arithmetic modulo 59.

3. Encode the following message

NUMBER THEORY IS AWESOME

using

- (a) a Caesar shift of -2 ;
- (b) a 3×4 permutation code;
- (c) a Vigenère code with the key word "PRIME".